Homeland Security Information Bulletin

Subject: Compromised Private Branch Exchange (PBX) and Telephone Voice Mail Systems
June 3, 2003

This Bulletin is being disseminated for information purposes only. The Department of Homeland Security is working with the Federal Bureau of Investigation to address multiple reports from private industry describing incidents involving compromises of Private Branch Exchange (PBX) and telephone voice-mail systems. These compromises allow unauthorized users to make long distance domestic and international telephone calls through the compromised systems.
FBI Field Offices in several cities have been working closely with fraud investigators from various telecommunication carriers who Have reported encountering intruders making numerous international calls.

A common scenario for these compromises follows this general pattern: An intruder circumvents a PBX system's security and gains access to a voice-mail system. The intruder may then configure the compromised system to dial out to a domestic or foreign phone number.

PBX compromises are not a new vulnerability, but they highlight the need for PBX users to maintain vigilance. These schemes appear to be becoming more prevalent. This illegal activity enables unauthorized individuals anywhere in the world to communicate via compromised US phone systems in a way that is difficult to trace. Reports have also surfaced suggesting that some of these unauthorized calls are being used to connect to local access numbers for internet service providers, thereby giving the caller free Internet service via a modem. An intruder gaining unauthorized access to several mailboxes can redirect repeated calls to a specific number, such as 911, and cause denial-of-service (DoS) activity.

While law enforcement and industry investigators work to mitigate these ongoing schemes and prosecute the responsible parties, DHS in coordination with the FBI has chosen to highlight this activity in order to raise awareness among users of PBXs to the possible risk associated with exploitation of the PBX vulnerability. DHS and the FBI recommend that phone system administrators review their internal security policies, enable all password protection functions, change default passwords and continually audit phone billing records to detect unauthorized activity. Users of PBX systems should consider protecting themselves by performing the following basic actions:

1.. Periodically change the phone system administrator and maintenance
passwords
2.. Lock users out after a limited number of failed attempts at accessing
password protected accounts
3.. Mandate that all users create their own passwords and change them periodically
4.. Ensure that passwords are as long as permitted by your system
5.. Properly secure or disable unnecessary features such as call forwarding or call transfer

6.. Assign someone as phone system/voice mail administrator and keep him/her informed of personnel changes.

The National Institute of Standards and Technology (NIST) makes available on its Web page NIST Special Publication 800-24 entitled "PBX Vulnerability Assessment - Finding Holes in Your PBX Before Someone Else Does." This provides generic PBX security methodology and vulnerability analysis. The report can be found at:

http://www.csrc.nist.gov/publications/nistpubs/800-24/sp800-24pbx.pdf

For specific security and vulnerability information, PBX administrators should consult with their respective PBX system vendor.

DHS encourages individuals to report information regarding suspicious or criminal activity to law enforcement or a Homeland Security watch office.
Individuals may report incidents online at
http://www.nipc.gov/incident/cirr.htm

Federal agencies/departments may report incidents online at
https://incidentreport.fedcirc.gov

Contact numbers for the IAIP watch centers are:
for private citizens and companies,
(202) 323-3205, 1-888-585-9078 or nipc.watch@fbi.gov ;
for the telecom industry, (703) 607-4950 or ncs@dhs.gov;
and for Federal agencies/departments, (888) 282-0870 or
fedcirc@fedcirc.gov.
Contactinformation for the FBI's field offices can be found at
http://www.fbi.gov/contact/fo/fo.htm

DHS intends to update this Bulletin should it receive additional relevant information, including information provided to it by the user community.

Based on this notification, no change to the Homeland Security Advisory Level is anticipated; the current HSAS level is YELLOW.